AMENDMENTS TO THE CLAIMS

Claim 1 (Currently Amended): An authentication token which is normally held by a user and, when the user is to use a device for executing predetermined processing in accordance with authentication data of the user, connected to the device to perform user authentication on the basis of biometrical information of the user, characterized by comprising:

a personal collation unit including a sensor for detecting the biometrical information of the user and outputting a detection result as sensing data, a storage unit which stores in advance registered data to be collated with the biometrical information of the user, and a collation unit for collating the registered data stored in said storage unit with the sensing data from said sensor and outputting a collation result as authentication data representing a user authentication result;

a communication unit for transmitting the authentication data from said personal collation unit to the device as communication data, and

a protocol conversion unit for converting [[data]] format of the communication data ~~from said communication unit~~ to be transmitted to the device into a ~~predetermined data~~ format that can be received and decoded by the device~~and transmitting the communication data to the device~~,

wherein said personal collation unit and communication unit are integrated.

Claim 2 (Previously Presented): The token according to claim 1, wherein

said storage unit further stores in advance user information unique to the user, which is to be used for processing in the device, and

said collation unit outputs the authentication data containing the user information read out from said storage unit.

Claim 3 (Canceled)

Claim 4 (Previously Presented): The token according to claim 1, further comprising a radio unit for transmitting the communication data from said communication unit to the device through a radio section.

Claim 5 (Previously Presented): The token according to claim 1, further comprising a radio unit for transmitting the communication data from said protocol conversion unit to the device through a radio section.

Claim 6 (Previously Presented): The token according to claim 1, further comprising a battery for supplying power.

Claim 7 (Previously Presented): The token according to claim 6, wherein said battery comprises a secondary battery charged by power supply from the device when said authentication token is connected to the device.

Claim 8 (Previously Presented): The token according to claim 1, wherein said storage unit has, in addition to a storage area for storing the registered data, at least one storage area for storing another information.

Claim 9 (Previously Presented): The token according to claim 7, wherein said at least one storage area for storing another information includes a storage area for storing personal information of the user and a storage area for storing service information.

Claim 10 (Currently Amended): An authentication system for executing user authentication, which is necessary for use of a device for executing predetermined processing, by using biometrical information of a user, characterized by comprising:

an authentication token which is normally held by the user and, when the user is to use said device, the authentication token connected to said device and to perform user authentication on the basis of the biometrical information of the user,

said authentication token comprising

a personal collation unit including a sensor for detecting the biometrical information of the user and outputting a detection result as sensing data, a storage unit which stores in advance registered data to be collated with the biometrical information of the user, and a collation unit for collating the registered data stored in said storage unit with the sensing data from said sensor and outputting a collation result representing a user authentication result as authentication data, [[and]]

a first communication unit for transmitting the authentication data from said personal collation unit to said device as communication data, and

a protocol conversion unit for converting format of the communication data to be transmitted to the device into a format that can be received and decoded by the device,

said personal collation unit and said first communication unit being integrated, and

said device comprising

a second communication unit for receiving the communication data transmitted from said authentication token and outputting the data as the authentication data, and

a processing unit for executing the predetermined processing on the basis of the collation result contained in the authentication data from said second communication unit.

Claim 11 (Previously Presented): The system according to claim 10, wherein said storage unit has a plurality of storage areas for storing not only the registered information of the user but also another information.

Claim 12 (Previously Presented): The system according to claim 10, wherein

said storage unit of said authentication token stores in advance user information unique to the user, which is to be used for processing in said device,

said collation unit of said authentication token outputs the authentication data containing the user information read out from said storage unit, and

said processing unit of said device executes processing using the user information contained in the authentication data from said second communication unit.

Claim 13 (Previously Presented): The system according to claim 10, further comprising a data conversion module connected to said authentication token to convert the communication data from said first communication unit of said authentication token into a predetermined data format and transmit the communication data to said device .

Claim 14 (Previously Presented): The system according to claim 10, wherein

said system further comprises a radio module connected to said authentication token to transmit the communication data from said first communication unit of said authentication token to said device through a radio section, and

said device comprises a radio unit for receiving the communication data transmitted from said radio module through the radio section and outputting the communication data to said second communication unit.

Claim 15 (Previously Presented): The system according to claim 13, wherein

said system further comprises a radio module connected to said authentication token to transmit the communication data from said data conversion module to said device through a radio section, and

said device comprises a radio unit for receiving the communication data transmitted from said radio module through the radio section and outputting the communication data to said second communication unit.

Claim 16 (Previously Presented): The system according to claim 10, wherein said authentication token further comprises a battery for supplying power into said authentication token.

Claim 17 (Previously Presented): The system according to claim 13, wherein said data conversion module further comprises a battery for supplying power into said data conversion module and authentication token.

Claim 18 (Previously Presented): The system according to claim 14, wherein said radio module further comprises a battery for supplying power into said radio module and authentication token.

Claim 19 (Previously Presented): The system according to claim 16, wherein said battery comprises a secondary battery charged by power supply from said device when said authentication token is connected to said device.

Claim 20 (Previously Presented): The token according to claim 1, wherein

said authentication token further comprises another storage circuit for storing a password of said authentication token and token identification information for identifying said authentication token, and

when the personal collation result indicates that the collation is successful, said communication unit transmits the password and token identification information in said another storage circuit to said service providing apparatus as the communication data.

Claim 21 (Currently Amended): An authentication system for executing user authentication, which is necessary when a user is to use a service providing apparatus for providing a predetermined service, by using biometrical information of the user, comprising:

an authentication token which is normally held by the user and, when the user is to use said service providing apparatus, connected to said service providing apparatus to perform user authentication on the basis of the biometrical information of the user,

said authentication token comprising a personal collation unit for performing collation on the basis of the biometrical information detected from the user to check whether the user is an authentic user, a storage circuit for storing a password of said authentication token and token identification information for identifying said authentication token, ~~and~~ a first communication unit for, when a collation result by said personal collation unit indicates that collation is successful, transmitting the password and token identification information in said storage circuit to said service providing apparatus as communication data, and a protocol conversion unit for converting format of the communication data to be transmitted to the service providing apparatus into a format that can be received and decoded by the service providing apparatus, and

said service providing apparatus comprising a second communication unit for receiving the communication data from said authentication token, a first database for storing the token identification information and password of said authentication token in advance in association with each other, a collation circuit for collating the password contained in the communication data with a password obtained from said first database using the token identification information as a key, and a processing unit for providing the service to the user on the basis of a collation result by said collation circuit.

Claim 22 (Previously Presented): The system according to claim 21, further comprising a registration apparatus connected to said service providing apparatus through a communication network to register the token identification information and password in said database in association with each other.

Claim 23 (Previously Presented): The system according to claim 21, wherein

said service providing apparatus has a password generation circuit for generating a new password and transmitting the new password to said authentication token through said second communication unit and updating the password stored in said first database , and

said first communication unit of said authentication token updates the password stored in said storage circuit by the new password received from said service providing apparatus.

Claim 24 (Previously Presented): The system according to claim 21, wherein

said service providing apparatus has a storage circuit for storing device identification information for identifying said service providing apparatus, and said second communication unit reads out the device identification information from said storage circuit and transmits the identification information to said authentication token when said authentication token is connected, and

said authentication token has a second database for storing the password and the device identification information for identifying the service providing apparatus in association with each other, and said first communication unit uses, as the password to be transmitted to said service providing apparatus, a password obtained from said second database using the device identification information received from said service providing apparatus as a key.

Claim 25 (Currently Amended): An authentication method of executing user authentication, which is necessary when a user is to use a service providing apparatus for providing a predetermined service, between the service providing apparatus and an authentication token for executing the user authentication using biometrical information of the user, characterized in that

the authentication token stores in advance a password of the authentication token and token identification information for identifying the authentication token, performs collation on the basis of the biometrical information detected from the user to check whether the user is an authentic user, and when a collation result indicates that collation is successful, ~~transmits~~converts formats of communication data containing the password and token identification information into a format that can be received and decoded by the service providing apparatus and transmits the communication data to the service providing apparatus ~~as communication data~~, and

the service providing apparatus stores the token identification information and password of the authentication token in advance in a first database in association with each other, collates the password contained in the communication data received from the authentication token with a password obtained from the first database using the token identification information as a key, and provides the service to the user on the basis of a collation result.

Claim 26 (Previously Presented): The method according to claim 25, wherein the token identification information and password are registered in the first database in association with each other from a registration apparatus connected to the service providing apparatus through a communication network.

Claim 27 (Previously Presented): The method according to claim 25, wherein

the service providing apparatus causes a password generation circuit to generate a new password, transmits the new password to the authentication token through the second communication unit, and updates the password stored in the first database, and

the authentication token updates the password stored in advance by the new password received from the service providing apparatus.

Claim 28 (Previously Presented): The method according to claim 25, wherein

the service providing apparatus stores device identification information for identifying the service providing apparatus in advance, and transmits the device identification information to the authentication token when the authentication token is connected, and

the authentication token stores in advance the password and the device identification information for identifying the service providing apparatus in a second database in association with each other, and uses, as the password to be transmitted to the service providing apparatus, a password obtained from the second database using the device identification information received from the service providing apparatus as a key.

Claim 29 (Currently Amended): A recording medium which stores a program for causing a computer to execute an authentication procedure of executing user authentication, which is necessary when a user is to use a service providing apparatus for providing a predetermined service, between the service providing apparatus and an authentication token for executing the user authentication using biometrical information of the user,

said program comprising:

in the service providing apparatus, storing token identification information and a password of the authentication token in a first database in advance in association with each other;

in the authentication token, after collation of the user based on the biometrical information detected from the user, and when a collation result indicates that collation is successful, receiving communication data containing the password of the authentication token and the token identification information for identifying the authentication token, which is transmitted ~~for~~ from the authentication token;

collating the password contained in the communication data with a password obtained from the first database using the token identification information as a key; and

providing the service to the user on the basis of a collation result,

wherein format of said communication data transmitted from the authentication token is converted into a format that can be received and decoded by the service providing apparatus.

Claim 30 (Previously Presented): The medium according to claim 29, wherein said program further comprises, in the service providing apparatus, registering the token identification information and password in the first database in association with each other from a registration apparatus connected to the service providing apparatus through a communication network.

Claim 31 (Previously Presented): The medium according to claim 29, wherein said program further comprises:

in the service providing apparatus, causing a password generation circuit to generate a new password;

transmitting the new password to the authentication token through the second communication unit so as to update the password stored in the authentication token in advance; and

updating the password stored in the first database by the new password.

Claim 32 (Previously Presented): The medium according to claim 29, wherein said program further comprises:

in the service providing apparatus, storing device identification information for identifying the service providing apparatus in advance; and

transmitting the device identification information to the authentication token when the authentication token is connected so as to store the password and the device identification information used to identify the service providing apparatus in the authentication token in a second database in association with each other, and searching the second database for a password using the device identification information received from the service providing apparatus as a key as the password to be transmitted to the service providing apparatus.

Claim 33 (Currently Amended): A program for causing a computer to execute an authentication procedure of executing user authentication, which is necessary when a user is to use a service providing apparatus for providing a predetermined service, between the service providing apparatus and an authentication token for executing the user authentication using biometrical information of the user, said program causing the computer to:

in the service providing apparatus, store token identification information and a password of the authentication token in a first database in advance in association with each other;

in the authentication token, after collation of the user based on the biometrical information detected from the user, and when a collation result indicates that collation is successful, receive communication data containing the password of the authentication token and the token identification information for identifying the authentication token, which is transmitted ~~for~~ from the authentication token;

collate the password contained in the communication data with a password obtained from the first database using the token identification information as a key; and

provide the service to the user on the basis of a collation result, wherein format of said communication data transmitted from the authentication token is converted into a format that can be received and decoded by the service providing apparatus.

Claim 34 (Currently Amended): The program according to claim 33, said program further causing the computer to, in the service providing apparatus, register[[ing]] the token identification information and password in the first database in association with each other from a registration apparatus connected to the service providing apparatus through a communication network.

Claim 35 (Currently Amended): The program according to claim 33, said program further causing the computer to:

in the service providing apparatus, cause a password generation circuit to generate a new password;

transmit[[ting]] the new password to the authentication token through the second communication unit so as to update the password stored in the authentication token in advance; and

update the password stored in the first database by the new password.

Claim 36 (Currently Amended): The program according to claim 33, said program further causing the computer to:

in the service providing apparatus, store device identification information for identifying the service providing apparatus in advance; and

transmit[[ting]] the device identification information to the authentication token when the authentication token is connected so as to store the password and the device identification information used to identify the service providing apparatus in the authentication token in a second database in association with each other, and searching the second database for a password using the device identification information received from the service providing apparatus as a key as the password to be transmitted to the service providing apparatus.

Claims 37-50 (Canceled):

Claim 51 (Withdrawn): A gate opening/closing system for opening/closing an entrance gate for a site, characterized by comprising:

an authentication token (306) for authenticating a user on the basis of biometrical information of the user;

a database (302) for storing identification information of the user when the user prepays an admission to the site; and

control means (303) for, when said authentication token authenticates that the user is an authentic user, and the identification information of the user, which is stored in said authentication token in advance, is output from said authentication token at the time of entrance of the user to the site, receiving the identification information, and when the received identification information has been stored in said database, opening the entrance gate.

Claim 52 (Withdrawn): A gate opening/closing system for opening/closing an entrance gate for a site, characterized by comprising:

information transmission/reception means for transmitting/receiving information to/from an authentication token which stores identification information of a user;

a database for storing the identification information of the user when the user prepays an admission to the site; and

control means for opening the entrance gate when said authentication token authenticates that the user is an authentic user on the basis of biometrical information of the user, the identification information of the user, which is output from said authentication token, is received by said information transmission/reception means at the time of entrance of the user to the site, and the received identification information has been stored in said database.

Claim 53 (Withdrawn): A system according to claim 51, wherein

said authentication token is a fingerprint authentication token for authenticating the user on the basis of fingerprint information of the user, and comprises

storage means for storing the fingerprint information of the user,

a fingerprint sensor for detecting a fingerprint of the user, and

processing means for authenticating the user as the authentic user on the basis of matching between detected information from said fingerprint sensor and stored information in said storage means.

Claim 54 (Withdrawn): A system according to claim 52, wherein

said authentication token is a fingerprint authentication token for authenticating the user on the basis of fingerprint information of the user, and comprises

storage means for storing the fingerprint information of the user,

a fingerprint sensor for detecting a fingerprint of the user, and

processing means for authenticating the user as the authentic user on the basis of matching between detected information from said fingerprint sensor and stored information in said storage means.

Claim 55 (Withdrawn): A system according to claim 51, further comprising identification information assignment means for, when said fingerprint authentication token is inserted, and the user prepays the admission to the site, generating a password and causing said fingerprint authentication token to store the password as the identification information, and transmitting the password to said database and causing said database to store the password as the identification information of the user.

Claim 56 (Withdrawn): A system according to claim 52, further comprising identification information assignment means for, when said fingerprint authentication token is inserted, and the user prepays the admission to the site, generating a password and causing said fingerprint authentication token to store the password as the identification information, and transmitting the password to said database and causing said database to store the password as the identification information of the user.

Claim 57 (Withdrawn): A system according to claim 51, wherein

said fingerprint authentication token stores an identification number of the user as the identification information in advance, and

said system further comprises identification information assignment means for, when said fingerprint authentication token is inserted, and the user prepays the admission to the site, reading the identification information from the fingerprint authentication token, transmitting the identification information to said database, and causing said database to store the identification information as the identification information of the user.

Claim 58 (Withdrawn): A system according to claim 52, wherein

said fingerprint authentication token stores an identification number of the user as the identification information in advance, and

said system further comprises identification information assignment means for, when said fingerprint authentication token is inserted, and the user prepays the admission to the site, reading the identification information from the fingerprint authentication token, transmitting the identification information to said database, and causing said database to store the identification information as the identification information of the user.

Claim 59 (Withdrawn): A system according to claim 51, further comprising

transmission means for converting identification information added to said authentication token and output from said authentication token into a radio signal or infrared signal and transmitting the signal, and

reception means, arranged near the entrance gate, for, upon receiving the radio signal or infrared signal transmitted by said transmission means, sending the identification information contained in the received radio signal or infrared signal to said control means.

Claim 60 (Withdrawn): A system according to claim 52, further comprising

transmission means for converting identification information added to said authentication token and output from said authentication token into a radio signal or infrared signal and transmitting the signal, and

reception means, arranged near the entrance gate, for, upon receiving the radio signal or infrared signal transmitted by said transmission means, sending the identification information contained in the received radio signal or infrared signal to said control means.

Claim 61 (Withdrawn): A biometrical information authentication automatic teller machine for providing, to a user, a service including deposit/withdrawal of cash for the user on the basis of authentication of biometrical information of the user, characterized by comprising:

a biometrical information authentication token for authenticating the user on the basis of the biometrical information of the user,

said biometrical information authentication token (1) comprising

storage means (12) for storing the biometrical information of the user,

a sensor (11) for detecting the biometrical information of the user, and

processing means (13) for outputting control information on the basis of matching between detected information from said sensor and stored information in said storage means, and

said biometrical information authentication automatic teller machine (401) comprising service providing means for providing the service to the user on the basis of the control information from said processing means.

Claim 62 (Withdrawn): A machine according to claim 61, wherein

said machine further comprises a database (410) which stores an outstanding balance corresponding to an account number of the user in advance,

said storage means of said biometrical information authentication token stores the account number of the user,

said processing means outputs the account number in said storage means as the control information on the basis of matching between the detected information from said sensor and the stored information in said storage means, and

said service providing means comprises

acquisition means for, upon receiving the account number from said processing means, acquiring the outstanding balance corresponding to the received account number from said database,

withdrawal means for withdrawing cash corresponding to predetermined operation by the user from the outstanding balance acquired by said acquisition means, and

outstanding balance recording means for subtracting an amount withdrawn by said withdrawal means from the outstanding balance acquired by said acquisition means and storing a new outstanding balance in said database.

Claim 63 (Withdrawn): A machine according to claim 61, wherein

said machine further comprises a database which stores an outstanding balance corresponding to an account number of the user in advance,

said storage means of said biometrical information authentication token stores the account number of the user,

said processing means outputs the account number in said storage means as the control information on the basis of matching between the detected information from said sensor and the stored information in said storage means, and

said service providing means comprises

acquisition means for, upon receiving the account number from said processing means, acquiring the outstanding balance corresponding to the received account number from said database, and outstanding balance recording means for adding an amount deposited by the user to the outstanding balance acquired by said acquisition means and storing a new outstanding balance in said database.

Claim 64 (Withdrawn): A biometrical information authentication automatic teller machine for providing, to a user, a service including deposit/withdrawal of cash for the user on the basis of authentication of biometrical information of the user, characterized by comprising:

information transmission/reception means for transmitting/receiving information to/from a biometrical information authentication token for authenticating the user on the basis of comparison/collation between biometrical information stored in storage means and the biometrical information of the user, which is detected by a sensor; and

service providing means for, when said information transmission/reception means receives control information output from the biometrical information authentication token on the basis of matching between detected information from the sensor and the biometrical information in the storage means, providing the service to the user on the basis of the received control information.

Claim 65 (Withdrawn): A machine according to claim 64, wherein

said machine further comprises a database which stores an outstanding balance corresponding to an account number of the user in advance,

the storage means of the biometrical information authentication token stores the account number of the user, and

said service providing means comprises

acquisition means for, when said information transmission/reception means receives the account number output from the biometrical information authentication token as the control information on the basis of matching between the detected information from the sensor and the biometrical information in the storage means, acquiring the outstanding balance corresponding to the received account number from said database,

withdrawal means for withdrawing cash corresponding to predetermined operation by the user from the outstanding balance acquired by said acquisition means, and outstanding balance recording means for subtracting an amount withdrawn by said withdrawal means from the outstanding balance acquired by said acquisition means and storing a new outstanding balance in said database.

Claim 66 (Withdrawn): A machine according to claim 64, wherein

said machine further comprises a database which stores an outstanding balance corresponding to an account number of the user in advance,

the storage means of the biometrical information authentication token stores the account number of the user, and

said service providing means comprises

acquisition means for, when said information transmission/reception means receives the account number output from the biometrical information authentication token as the control information on the basis of matching between the detected information from the sensor and the biometrical information in the storage means, acquiring the outstanding balance corresponding to the received account number from said database, and

outstanding balance recording means for adding an amount deposited by the user to the outstanding balance acquired by said acquisition means and storing a new outstanding balance in said database.

Claim 67 (Withdrawn): A machine according to claim 61, wherein when a passbook of the user is inserted, said outstanding balance recording means records information including the outstanding balance on the passbook.

Claim 68 (Withdrawn): A machine according to claim 64, wherein when a passbook of the user is inserted, said outstanding balance recording means records information including the outstanding balance on the passbook.

Claim 69 (Withdrawn): A machine according to claim 61, wherein

said storage means stores a fingerprint image of the user as the biometrical information,

said sensor detects the fingerprint image of the user as the biometrical information, and said processing means or biometrical information authentication token outputs the control information on the basis of matching between the fingerprint image detected by said sensor and the fingerprint image in said storage means.

Claim 70 (Withdrawn): A machine according to claim 69, wherein

the storage means stores a fingerprint image of the user as the biometrical information,

the sensor detects the fingerprint image of the user as the biometrical information, and

said processing means or biometrical information authentication token outputs the control information on the basis of matching between the fingerprint image detected by the sensor and the fingerprint image in the storage means.

Claim 71 (Withdrawn): A portable terminal system comprising a portable terminal device (501) and a biometrical authentication device (502), characterized in that

said biometrical authentication device (502) comprises

biometrical information read means (11) for reading biometrical information of a user who holds said biometrical authentication device,

first storage means (12) for storing biometrical information of an authentic user registered in advance and personal information of the authentic user, and

a first processing unit (13, 14) for performing personal authentication by collating the biometrical information read by said biometrical information read means (11) with the biometrical information of the authentic user stored in said first storage means (12), and only when an authentication result represents that collation is successful, transmitting the personal information stored in said first storage means to said portable terminal device, and

said portable terminal device (501) comprises

second storage means (515) for storing the personal information transmitted from said biometrical authentication device (502), and

second processing means (514) for executing communication processing or data processing using the personal information stored in said second storage means.

Claim 72 (Withdrawn): A portable terminal system comprising a portable terminal device (501) and a biometrical authentication device (502), characterized in that

said biometrical authentication device (502) comprises

biometrical information read means (11) for reading biometrical information of a user who holds said biometrical authentication device,

first storage means (12) for storing biometrical information of an authentic user registered in advance and service information necessary for the authentic user to receive a service, and

a first processing unit (13, 14) for performing personal authentication by collating the biometrical information read by said biometrical information read means with the biometrical information of the authentic user stored in said first storage means, and only when an authentication result represents that collation is successful, transmitting the service information stored in said first storage means to said portable terminal device, and

said portable terminal device (501) comprises

second storage means (515) for storing the service information transmitted from said biometrical authentication device (502), and

second processing means (514) for executing communication processing or data processing using the service information stored in said second storage means.

Claim 73 (Withdrawn): A system according to claim 71, wherein

the personal information contains a personal identification number of the authentic user, and

after the personal information is stored in said second storage means, said second processing means of said portable terminal device is connected to a network using the personal identification number contained in the personal information.

Claim 74 (Withdrawn): A system according to claim 72, wherein

the service information contains a password used to log in to a web site, and

after the service information is stored in said second storage means, said second processing means of said portable terminal device acquires, from the service information, a password corresponding to a web site accessed through a network and transmits the acquired password to the accessed web site.

Claim 75 (Withdrawn): A biometrical authentication device characterized by comprising:

biometrical information read means for reading biometrical information of a user who holds said device;

storage means for storing biometrical information of an authentic user registered in advance and personal information of the authentic user; and

a processing unit for performing personal authentication by collating the biometrical information read by said biometrical information read means with the biometrical information of the authentic user stored in said storage means, and only when an authentication result represents that collation is successful, transmitting the personal information stored in said storage means to a portable terminal device,

wherein only when the authentication result represents that the collation is successful, the personal information is transmitted to the portable terminal device which does not hold the personal information, thereby allowing communication processing or data processing using the personal information.

Claim 76 (Withdrawn): A biometrical authentication device characterized by comprising:

biometrical information read means for reading biometrical information of a user who holds said device;

storage means for storing biometrical information of an authentic user registered in advance and service information necessary for the authentic user to receive a service; and

a processing unit for performing personal authentication by collating the biometrical information read by said biometrical information read means with the biometrical information of the authentic user stored in said storage means, and only when an authentication result represents that collation is successful, transmitting the service information stored in said storage means to a portable terminal device,

wherein only when the authentication result represents that the collation is successful, the service information is transmitted to the portable terminal device which does not hold the service information, thereby allowing communication processing or data processing using the service information.

Claim 77 (Withdrawn): A device according to claim 75, wherein the personal information contains a personal identification number of the authentic user, which is necessary to connect the portable terminal device to a network.

Claim 78 (Withdrawn): A device according to claim 76, wherein the service information contains a password used to log in to a web site from the portable terminal device through a network.

Claim 79 (Withdrawn): A portable terminal device characterized by comprising:

storage means for receiving personal information of an authentic user from a biometrical authentication device and storing the personal information, the biometrical authentication device executing personal authentication using biometrical information of a user, and transmitting the personal information of the authentic user only when an authentication result indicates that collation is successful; and

processing means for executing communication processing or data processing using the personal information stored in said storage means,

wherein the communication processing or data processing using the personal information is executed only when the personal information stored in the biometrical authentication device is received.

Claim 80 (Withdrawn): A portable terminal device characterized by comprising:

storage means for receiving service information necessary for an authentic user to receive a service from a biometrical authentication device and storing the service information, the biometrical authentication device executing personal authentication using biometrical information of a user, and transmitting the service information only when an authentication result indicates that collation is successful; and processing means for executing communication processing or data processing using the service information stored in said storage means,

wherein the communication processing or data processing using the service information is executed only when the service information stored in the biometrical authentication device is received.

Claim 81 (Withdrawn): A device according to claim 79, wherein

the personal information contains a personal identification number of the authentic user, and

after the personal information is stored in said storage means, said processing means of said portable terminal device is connected to a network using the personal identification number contained in the personal information.

Claim 82 (Withdrawn): A device according to claim 80, wherein

the service information contains a password used to log in to a web site, and

after the service information is stored in said storage means, said processing means of said portable terminal device acquires, from the service information, a password corresponding to a web site accessed through a network and transmits the acquired password to the accessed web site.

Claim 83 (Currently Amended): A token according to claim 1, wherein

said token further comprises an encryption circuit for encrypting data generated from the authentication data and dynamic information generated by the **[[**use **]]**device and transmitted using a key registered in advance, and

said communication circuit transmits to the **[[**use **]]**device encrypted data generated by said encryption circuit,

wherein the dynamic information changes each time it is generated.

Claim 84 (Currently Amended): The token according to claim 1, wherein

said token further comprises

a result determination circuit for, when the collation result indicates that the authentication is successful, outputting the authentication data to said encryption circuit, and when the collation result indicates that the authentication fails, outputting the authentication data to said first communication circuit, and

an encryption circuit for, in accordance with the authentication data from said result determination circuit, encrypting dynamic information transmitted from the[[use]] device using a key registered in advance, adding obtained encrypted data to the authentication data, and outputting the encrypted data, and

said communication circuit transmits to the [[use]]device the authentication data with the encrypted data from said encryption circuit or the authentication data from said result determination circuit.

Claim 85 (Currently Amended): The token according to claim 1, wherein

said token further comprises

an encryption circuit for encrypting dynamic information transmitted from the[[use]] device using a key registered in advance and outputting obtained encrypted data to said first communication circuit as data, and

a first result determination circuit for, when the collation result indicates that the authentication is successful, instructing said encryption circuit to generate the encrypted data, and when the collation result indicates that the authentication fails, outputting data whose number of digits is different from that of the encrypted data that would be produced if the authentication was successful to said first communication circuit, and

said first communication circuit transmits to the [[use]]device the data from said encryption circuit or the data from said first result determination circuit.

Claim 86 (Currently Amended): The token according to claim 84, wherein

said token further comprises an ID storage circuit for storing identification information of said authentication token registered in advance, and

said first communication circuit transmits to the [[use]]device the identification information stored in said ID storage circuit.

Claim 87 (Currently Amended): The system according to claim 10, wherein said storage circuit stores, as the user information, personal information of the user and service information related to the service provided by the [[use]]device, and stores the personal information, service information, and registered information in separate storage areas.

Claim 88 (Currently Amended): The system according to claim 10, wherein

said authentication token further comprises an encryption circuit for encrypting dynamic information transmitted from the [[use]]device and data generated from the authentication data using a key registered in advance,

said first communication circuit transmits to the [[use]]device encrypted data generated by said encryption circuit, and

said processing unit comprises a dynamic information generation circuit for generating the dynamic information to be transmitted to said authentication token, a decryption circuit for decrypting the encrypted data transmitted from said authentication token using a key corresponding to the key, and a result determination circuit for executing the predetermined processing only when a collation result of the authentication data contained in the data decrypted by said decryption circuit indicates that the authentication is successful, and the dynamic information contained in the data matches the dynamic information generated by said dynamic information generation circuit and transmitted to said authentication token.

Claim 89 (Currently Amended): The system according to claim 10, wherein

said authentication token further comprises a first result determination circuit for, when the collation result indicates that the authentication is successful, outputting the authentication data to said encryption circuit, and when the collation result indicates that the authentication fails, outputting the authentication data to said first communication circuit, and an encryption circuit for, in accordance with the authentication data from said first result determination circuit, encrypting dynamic information transmitted from the [[use]]device using a key registered in advance, adding obtained encrypted data to the authentication data, and outputting the encrypted data, said first communication circuit transmits to the [[use]]device the authentication data with the encrypted data from said encryption circuit or the authentication data from said first result determination circuit, and

said processing unit comprises a dynamic information generation circuit for generating the dynamic information to be transmitted to said authentication token, a decryption circuit for decrypting the encrypted data transmitted from said authentication token using a key corresponding to the key, and a second result determination circuit for causing said decryption circuit to decrypt the encrypted data added to the authentication data only when an authentication result of the authentication data from said authentication token, which is received by said second communication circuit, indicates that the authentication is successful, and executing the predetermined processing only when the obtained dynamic information matches the dynamic information generated by said dynamic information generation circuit and transmitted to said authentication token.

Claim 90 (Currently Amended): The_system according to claim 10, wherein

said authentication token further comprises an encryption circuit for encrypting dynamic information transmitted from the [[use]]device using a key registered in advance and outputting obtained encrypted data to said first communication circuit as data, and a first result determination circuit for, when the collation result indicates that the authentication is successful, instructing said encryption circuit to generate the encrypted data, and when the collation result indicates that the authentication fails, outputting data whose number of digits is different from that of the encrypted data to said first communication circuit,

said first communication circuit transmits to the [[use]]device the data from said encryption circuit or the data from said first result determination circuit, and

said processing unit comprises a dynamic information generation circuit for generating the dynamic information to be transmitted to said authentication token, a decryption circuit for decrypting the encrypted data transmitted from said authentication token using a key corresponding to the key, and a second result determination circuit for causing said decryption circuit to decrypt the encrypted data added to the data only when the number of digits of the data from said authentication token, which is received by said second communication circuit, indicates the number of digits when the authentication is successful, and executing the predetermined processing only when the obtained dynamic information matches the dynamic information generated by said dynamic information generation circuit and transmitted to said authentication token.

Claim 91 (Currently Amended): The system according to claim 88, wherein

said authentication token further comprises an ID storage circuit for storing identification information of said authentication token registered in advance,

said first communication circuit transmits to the [[use]]device the identification information stored in said ID storage circuit, and

said decryption circuit decrypts the encrypted data from said authentication token using a key corresponding to the identification information transmitted from said authentication token.

Claim 92 (Currently Amended): The system according to claim 89, wherein

said authentication token further comprises an ID storage circuit for storing identification information of said authentication token registered in advance,

said first communication circuit transmits to the [[use]]device the identification information stored in said ID storage circuit, and

said decryption circuit decrypts the encrypted data from said authentication token using a key corresponding to the identification information transmitted from said authentication token.

Claim 93 (Currently Amended): The system according to claim 90, wherein

said authentication token further comprises an ID storage circuit for storing identification information of said authentication token registered in advance,

said first communication circuit transmits to the [[use]]device the identification information stored in said ID storage circuit, and

said decryption circuit decrypts the encrypted data from said authentication token using a key corresponding to the identification information transmitted from said authentication token.

Claim 94 (New): A biometrical information authentication storage which locks or unlocks a door of a main body in storing an article in the main body or taking out the article stored in the main body, and also unlocks the door on the basis of authentication of biometrical information of a user, comprising:

drive means for locking/unlocking the door;

storage means for storing the biometrical information of the user, said storage means stores a fingerprint image of the user as the biometrical information, each user has a fingerprint authentication token; and

processing means for controlling said drive means to unlock the door on the basis of matching between stored information in said storage means and detected information from a sensor for detecting the biometrical information of the user, said processing means controls said drive means to unlock the door on the basis of matching between the stored information in said storage means and the fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, said processing means comprises

lock means for, when the fingerprint authentication token is inserted into the main body in storing the article in the main body, controlling said drive means to lock the door, generating a new password whenever the door is locked, storing the password in said storage means, transmitting the password to the fingerprint authentication token, and causing the fingerprint authentication token to store the password, and

unlock means for controlling said drive means to unlock the door when a password based on matching between a registered fingerprint image and the fingerprint image detected by the sensor and output from the fingerprint authentication token is received in taking out the article stored in the main body, and the received password matches the password in said storage means,

wherein the fingerprint authentication token is independent of the main body and physically separated from the main body.

Claim 95 (New): A biometrical information authentication storage which locks or unlocks a door of a main body in storing an article in the main body or taking out the article stored in the main body, and also unlocks the door on the basis of authentication of biometrical information of a user, comprising:

drive means for locking/unlocking the door;

storage means for storing the biometrical information of the user, said storage means stores a fingerprint image of the user as the biometrical information, each user has a fingerprint authentication token, said storage further comprises

a plurality of storage sections capable of independently storing articles and having corresponding doors,

designation means for designating one of the plurality of doors, and

display means for displaying a number of the door;

processing means for controlling said drive means to unlock the door on the basis of matching between stored information in said storage means and detected information from a sensor for detecting the biometrical information of the user, said processing means controls said drive means to unlock the door on the basis of matching between the stored information in said storage means and the fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, said processing means comprises

first display control means for, when a corresponding door is closed in storing an article in a storage section, displaying the number of the door on said display means,

lock means for, when the door number displayed on said display means is designated by said designation means, and the fingerprint authentication token is inserted into the main body, controlling said drive means to lock the door, generating a new password whenever the door is locked, storing the password and the door number in said storage means, transmitting the password and the door number to the fingerprint authentication token, and causing the fingerprint authentication token to store the password and the door number,

second display control means for, when the fingerprint authentication token is inserted into the main body in taking out the article stored in said storage section, displaying the door number stored in the fingerprint authentication token on said display means, and

unlock means for controlling said drive means to unlock the door when the door number displayed on said display means is designated by said designation means, and a

password based on matching between a registered fingerprint image and the fingerprint image detected by the sensor and output from the fingerprint authentication token is received, and the received password matches the password in said storage means,
wherein the fingerprint authentication token is independent of the main body and physically separated from the main body.

Claim 96 (New): A lock/unlock method for a biometrical information authentication storage which locks or unlocks a door of a main body in storing an article in the main body or taking out the article stored in the main body, and also unlocks the door on the basis of authentication of biometrical information of a user, comprising:

a first step of unlocking the door on the basis of matching between stored information stored in storage means in advance and detected information from a sensor for detecting the biometrical information of the user, the storage means stores a fingerprint image of the user as the biometrical information, each user has a fingerprint authentication token; and

processing the first step comprises a second step of unlocking the door on the basis of matching between the stored information in the storage means and a fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, processing in the second step comprises

a third step of, when the fingerprint authentication token is inserted into the main body in storing the article in the main body, locking the door, generating a new password whenever the door is locked, storing the password in the storage means, transmitting the password to the fingerprint authentication token, and causing the fingerprint authentication token to store the password, and

a fourth step of unlocking the door when a password based on matching between a registered fingerprint image and the fingerprint image detected by the sensor and output from the fingerprint authentication token is received in taking out the article stored in the main body, and the received password matches the password in the storage means,
wherein the token is independent of the main body and physically separated from the main body.

Claim 97 (New): A lock/unlock method for a biometrical information authentication storage which locks or unlocks a door of a main body in storing an article in the main body or taking out the article stored in the main body, and also unlocks the door on the basis of authentication of biometrical information of a user, comprising:

a first step of unlocking the door on the basis of matching between stored information stored in storage means in advance and detected information from a sensor for detecting the biometrical information of the user, the storage means stores a fingerprint image of the user as the biometrical information, each user has a fingerprint authentication token, the storage means further comprises a plurality of storage sections capable of independently storing articles and having corresponding doors; and

processing the first step comprises a second step of unlocking the door on the basis of matching between the stored information in the storage means and a fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, processing in the second step comprises

a third step of, when a corresponding door is closed in storing an article in a storage section, displaying a number of the door,

a fourth step of, when the door number displayed on the basis of processing in the third step is designated, and the fingerprint authentication token is inserted into the main body, locking the door, generating a new password whenever the door is locked, storing the password and the door number in the storage means, transmitting the password and the door number to the fingerprint authentication token, and causing the fingerprint authentication token to store the password and the door number,

a fifth step of, when the fingerprint authentication token is inserted into the main body in taking out the article stored in the storage section, displaying the door number stored in the fingerprint authentication token, and

a sixth step of unlocking the door when the door number displayed on the basis of processing in the fifth step is designated, and a password based on matching between a registered fingerprint image and the fingerprint image detected by the sensor and output from the fingerprint authentication token is received, and the received password matches the password in the storage means, wherein the token is independent of the main body and physically separated from the main body.

Claim 98 (New): A biometrical information authentication storage which locks or unlocks a door of a main body in storing an article in the main body or taking out the article stored in the main body, and also unlocks the door on the basis of authentication of biometrical information of a user, comprising:

drive means for locking/unlocking the door;

storage means for storing the biometrical information of the user, said storage means stores a fingerprint image of the user as the biometrical information, each user has a fingerprint authentication token; and

processing means for controlling said drive means to unlock the door on the basis of matching between stored information in said storage means and detected information from a sensor for detecting the biometrical information of the user, said processing means controls said drive means to unlock the door on the basis of matching between the stored information in said storage means and the fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, said processing means comprises

lock means for, when a password generated by the fingerprint authentication token based on matching between a registered fingerprint image and the fingerprint image detected by the sensor is received in storing the article in the main body, controlling said drive means to lock the door, and storing the received password in said storage means, and

unlock means for controlling said drive means to unlock the door when the password based on matching between the registered fingerprint image and the fingerprint image detected by the sensor and output from the fingerprint authentication token is received in taking out the article stored in the main body, and the received password matches the password in said storage means

wherein the fingerprint authentication token is independent of the main body and physically separated from the main body.

Claim 99 (New): A lock/unlock method for a biometrical information authentication storage which locks or unlocks a door of a main body in storing an article in the main body or taking out the article stored in the main body, and also unlocks the door on the basis of authentication of biometrical information of a user, comprising:

the first step of unlocking the door on the basis of matching between stored information stored in storage means in advance and detected information from a sensor for detecting the biometrical information of the user, the storage means stores a fingerprint image of the user as the biometrical information, wherein each user has a fingerprint authentication token; and

processing the first step comprises a second step of unlocking the door on the basis of matching between the stored information in the storage means and a fingerprint image from the fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, the token is independent of the main body and physically separated from the main body,

wherein processing in the second step comprises

a third step of, when a password generated by the fingerprint authentication token based on matching between a registered fingerprint image and the fingerprint image detected by the sensor is received in storing the article in the main body, controlling drive means to lock the door, and storing the received password in said storage means, and

a fourth step of unlocking the door when the password based on matching between the registered fingerprint image and the fingerprint image detected by the sensor and output from the fingerprint authentication token is received in taking out the article stored in the main body, and the received password matches the password in the storage means.